UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 4:21-mj-07

21-006-04

REDACTED APPLICATION FOR SEARCH AND SEIZURE WARRANT

I, Craig Scherer, being first duly sworn, hereby depose and state as follows:

I am a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) in Sioux Falls, South Dakota, and have reason to believe that upon the person and within the property fully described in Attachment A, attached hereto and incorporated herein by reference, there is now concealed certain information, namely: that fully described in Attachment B, attached hereto and incorporated herein by reference, which I believe is property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, concerning violations of Title 21 U.S.C. §§ 841 and 846 (conspiracy to possess with intent to distribute a controlled substance) and 18 U.S.C. § 1956 (money laundering).

The facts to support a finding of Probable Cause are contained in my Affidavit filed herewith.

Craig Scherer, Special Agent
Department of Homeland Security

Sworn to and subscribed before me, telephonically, on the 11th day of January, 2021, at Sioux Falls, South Dakota.

VERONICA L. DUFFY
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 4:21-mj-07

21-006-04

REDACTED SEARCH AND SEIZURE WARRANT

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement officer or an attorney for the government requests the search of the person and property described in Attachment A, attached hereto and incorporated herein by reference.

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the property described above for the information fully described in Attachment B, attached hereto and incorporated herein by reference, and that such search will reveal evidence of the violations of 21 U.S.C. §§ 841 and 846 (possession and distributing or dispensing controlled substances or conspiracy to distribute or dispense a controlled substance) and 18 U.S.C. § 1956 (money laundering).

YOU ARE COMMANDED to execute this warrant on or before 1-25-2021 (not to exceed 14 days)
☒ in the daytime – 6:00 a.m. to 10:00 p.m.
☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the undersigned Judge.

1-11-2021 at 9:24 am CST at Sioux Falls, South Dakota
Date and Time Issued Telephonically

Veronica L Duffy

VERONICA L. DUFFY
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding	No. 4:21-mj-07
21-006-04	**REDACTED RETURN**

Date and time warrant executed: _____

Copy of warrant and inventory left with: _____

Inventory made in the presence of: _____

Inventory of the property taken and name of any person(s) seized (attach additional sheets, if necessary):

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

_____
Craig Scherer, Special Agent
Department of Homeland Security

REDACTED ATTACHMENT A

This warrant applies to information associated with the following [redacted] account [redacted], that are stored at premises owned, maintained, controlled, or operated by [redacted] a business with offices located at [redacted]

REDACTED ATTACHMENT B

I. Files and Accounts to be produced by [redacted]

To the extent that the information described in Attachment A is within the possession, custody, or control of [redacted] including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to [redacted] is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments);

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages ([redacted] SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the

actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on [redacted], including all [redacted] device backups, all [redacted] and third-party app data, all files and other records related to [redacted] Photo Sharing, My Photo Stream [redacted] Photo Library [redacted] Drive, [redacted] (including Pages, Numbers, and Keynote), [redacted]

f. The activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs [redacted]

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications [redacted] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the email accounts described in Attachment A, which is evidence, fruits, and instrumentalities of violations of Title 21 U.S.C. §§ 841 and 846 and 18 U.S.C. § 1956, including:

a. Images, videos and other files depicting the purchase, possession, transport, shipping and/or distribution of controlled substances, to include the receipt, possession and/or transfer of proceeds.

b. Communications or documentations regarding the purchase, possession, transport, shipping and/or distribution of controlled substances, to include the receipt, possession and/or transfer of proceeds.

c. Lists of customers and contacts and related identifying information.

d. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.

e. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).

f. Any information recording schedule or travel.

g. All financial records, [redacted].

h. Information pertaining to assets owned or under the control of the owners of the accounts being searched, including but not limited to Vehicle Identification Numbers (VINs), serial numbers and/or other identification numbers of assets.

i. Information related to firearms and ammunition.

j. Photographs and/or videos, in particular, photographs and/or videos of co-conspirators, assets and controlled substances.

k. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

l. Passwords and encryption keys, and other access information that may be necessary to access the account or identifiers listed on Attachment A and other associated accounts.

m. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while

minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 4:21-mj-07

21-006-04

REDACTED AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT

STATE OF SOUTH DAKOTA)
:SS
COUNTY OF MINNEHAHA)

I, Craig Scherer, being duly sworn on oath, depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) in Sioux Falls, South Dakota and have been duly employed in this position since December 2003. I am a graduate of the Criminal Investigator Training Program and ICE Special Agent Training Program at the Federal Law Enforcement Training Center. I have received specialized training pertaining to conducting criminal investigations, immigration and customs laws, investigative techniques, searching databases, conducting interviews, executing search warrants, and making arrests with respect to criminal violations of United States Code.

2. As a Special Agent one of my responsibilities is investigating drug trafficking organizations and associated money laundering methods. I have assisted with numerous investigations into violations of the Federal Controlled Substances Act and I am familiar with the provisions of Title 21 and 18 of the United States Code. I have been working drug trafficking cases since 2005.

PURPOSE OF AFFIDAVIT

3. Through this affidavit, I am requesting a search warrant be issued for all contents of the Apple account associated with [redacted] ("SUBJECT ACCOUNT"), that are stored at premises owned, maintained, controlled, or operated [redacted].

4. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNT constitutes evidence or instrumentalities of criminal violations [redacted].

5. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of United States Code are located within the accounts described in this affidavit.

6. I have received information from other law enforcement officers and sources of information by either verbal or written report. The officers and sources providing information may have received the information by way of personal knowledge or from another source.

SUMMARY OF INVESTIGATION

7. [redacted].

8. [redacted].

9. [redacted].

10. [redacted]

[redacted].

11. [redacted].

12. [redacted].

13. [redacted].

14. [redacted]:

- [redacted])
- [redacted].

- [redacted].

15. On [redacted].

16. [redacted].

17. [redacted].

18. [redacted].

19. On November [redacted].

20. [redacted].

21. On [redacted].

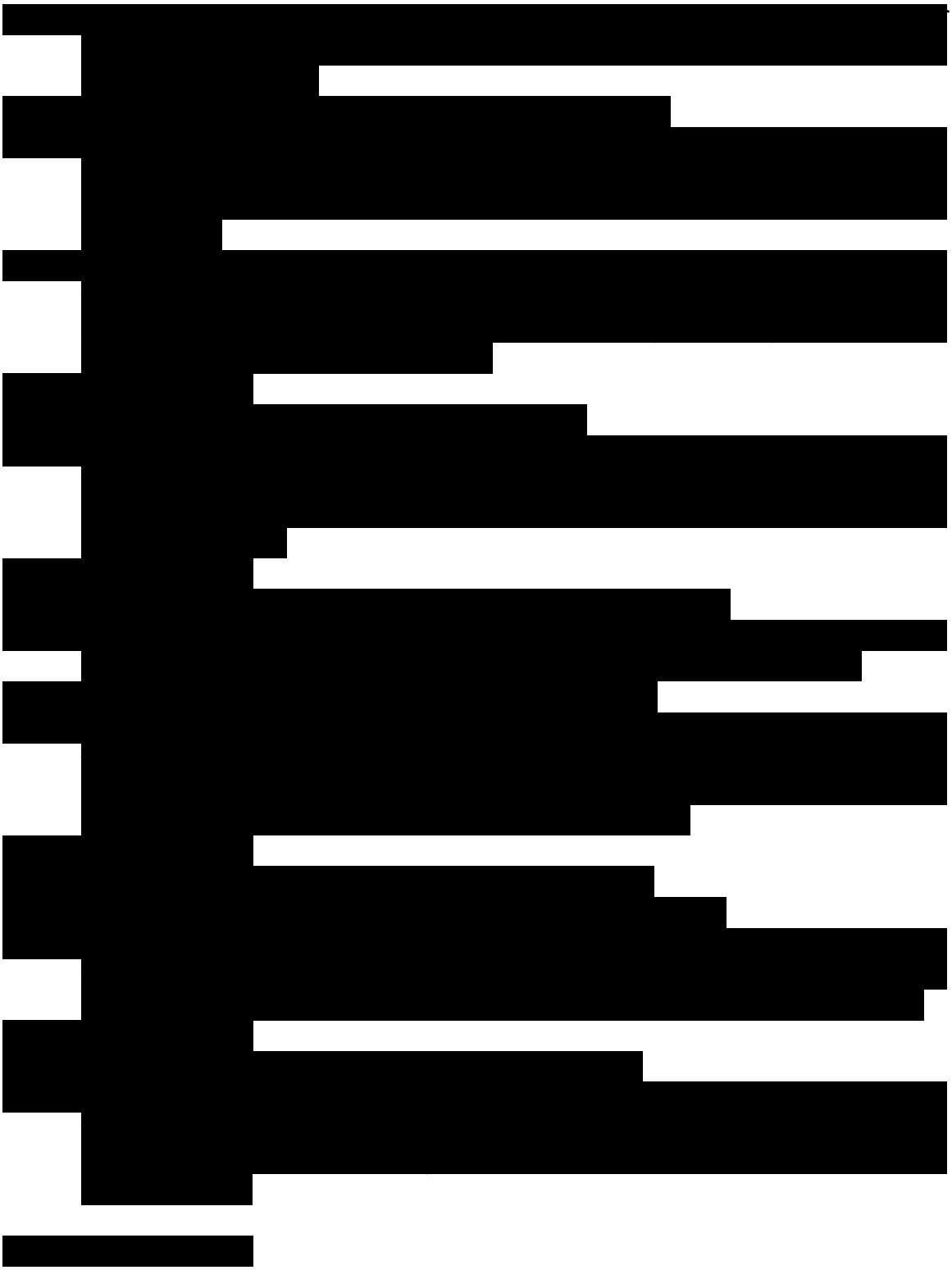
22. On [redacted].

[redacted]

- [redacted].

23. [redacted]:

[redacted]



[redacted]

- [redacted]

24. On [redacted].

25. [redacted]

[redacted].

26. [redacted].

27. [redacted].

28. [redacted].

29. [redacted],

[redacted].

30. [redacted].

31. [redacted]:

[redacted]

32. [redacted]8.

33. [redacted].

34. [redacted].

35. [redacted].

36. [redacted].

37. [redacted].

TECHNICAL BACKGROUND

[redacted]

39. [redacted].

40. [redacted].

[redacted].

41. [redacted].

42. [redacted]).

43. [redacted].

44. [redacted].

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

j. [redacted]

46. Based on my training and experience, I know that it is common for people involved in the sale, distribution, and use of illegal drugs to keep records of their customers and suppliers, sometimes in electronic devices.

47. I know based on my training and experience that even if long-time drug traffickers stop distributing controlled substances, either voluntarily or under law enforcement pressure, these traffickers often retain in their possession many items with evidentiary value, including telephones and telephone records; names, addresses and telephone numbers of associates; documents related to financial transactions; and other items as listed in this affidavit.

48. I know that computers and electronic storage devices may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime,

and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. In this case, I request permission to search the contents and all electronically stored information within the above-described accounts.

49. I believe based on the above information that individuals known and unknown are involved in drug trafficking activities and associated financial violations.

CONCLUSION

50. I respectfully request a search warrant be issued to search all contents and electronically stored information within the above-described accounts, for evidence of [redacted] as more fully described in Attachment A hereto.

51. Based on the foregoing, I request that the Court issue the requested search warrant.

Special Agent Craig Scherer
Homeland Security Investigations

Sworn to before me, and subscribed ~~in my presence~~ telephonically on the 11th day of January, 2021, at Sioux Falls, South Dakota.

VERONICA L. DUFFY
United States Magistrate Judge

REDACTED ATTACHMENT A

This warrant applies to information associated with the following [redacted] account [redacted], that are stored at premises owned, maintained, controlled, or operated by [redacted] a business with offices located at [redacted]

REDACTED ATTACHMENT B

I. Files and Accounts to be produced by [redacted]

To the extent that the information described in Attachment A is within the possession, custody, or control of [redacted] including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to [redacted] is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments);

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages ([redacted] SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the

actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on [redacted], including all [redacted] device backups, all [redacted] and third-party app data, all files and other records related to [redacted] Photo Sharing, My Photo Stream [redacted] Photo Library [redacted] Drive, [redacted] (including Pages, Numbers, and Keynote), [redacted]

f. The activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs [redacted]

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications [redacted] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the email accounts described in Attachment A, which is evidence, fruits, and instrumentalities of violations of Title 21 U.S.C. §§ 841 and 846 and 18 U.S.C. § 1956, including:

a. Images, videos and other files depicting the purchase, possession, transport, shipping and/or distribution of controlled substances, to include the receipt, possession and/or transfer of proceeds.

b. Communications or documentations regarding the purchase, possession, transport, shipping and/or distribution of controlled substances, to include the receipt, possession and/or transfer of proceeds.

c. Lists of customers and contacts and related identifying information.

d. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.

e. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).

f. Any information recording schedule or travel.

g. All financial records, [redacted].

h. Information pertaining to assets owned or under the control of the owners of the accounts being searched, including but not limited to Vehicle Identification Numbers (VINs), serial numbers and/or other identification numbers of assets.

i. Information related to firearms and ammunition.

j. Photographs and/or videos, in particular, photographs and/or videos of co-conspirators, assets and controlled substances.

k. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

l. Passwords and encryption keys, and other access information that may be necessary to access the account or identifiers listed on Attachment A and other associated accounts.

m. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while

minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.